



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/987,911	11/16/2001	Mark Crosbie	10012198	7932
7590	03/07/2005		EXAMINER	
HEWLETT-PACKARD COMPANY Intellectual Property Administration P.O. Box 272400 Fort Collins, CO 80527-2400			ANANTHANARAYANAN, RAMYA	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 03/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/987,911	CROSBIE ET AL.	
	Examiner Ramya Ananthanarayanan	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 16 November 2001.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-12 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-12 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____

1. Claims 1-12 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1 - 12 are rejected under 35 U.S.C. 102(b) as being anticipated by Kim et al. ("The Design and Implementation of Tripwire: A File System Integrity Checker").

4. With respect to claim 1, Kim et al. disclose a method of detecting critical file changes, comprising:

Reading events representing various types of system calls (page 27, Section 5.3, paragraph 1, lines 1-3);

Routing the event to an appropriate template, the event having multiple parameters (page 27, Section 5.3, paragraph 1, lines 1-3; page 24, Section 4.2, paragraph 3 till column end);

Filtering the event as either a possible intrusion based on the multiple parameters and either dropping the event or outputting the event (page 25, column 1, paragraph 1, lines 1-5); and

Creating an intrusion alert if an event is output from said filtering step (page 25, column 1, paragraph 1, lines 1-5).

5. With respect to claim 7, Kim et al. disclose a method of detecting critical file changes, comprising:

Reading events including encoded information representing system calls (page 27, Section 5.3, paragraph 1, lines 1-3; page 23, column 2, lines 7-8);
Routing the event to an appropriate template based on the encoded information (page 27, Section 5.3, paragraph 1, lines 1-3; page 24, Section 4.2, paragraph 3 till column end; page 23, column 2, lines 7-8);

Filtering the event as either a possible intrusion based on the encoded information and either dropping the event or outputting the event (page 25, column 1, paragraph 1, lines 1-5; page 23, column 2, lines 7-8); and

Creating an intrusion alert of an event is output from said filtering step (page 25, column 1, paragraph 1, lines 1-5; page 23, column 2, lines 7-8).

6. With respect to claims 2 and 8, Kim et al. disclose a method, wherein said filtering step outputs an event if the parameters indicate that the permission bits on a file or directory were changed (page 24, Section 4.2, paragraph 2, lines 1-4).

7. With respect to claims 3 and 9, Kim et al. disclose a method, wherein said filtering step outputs an event if the parameters indicate that a file was opened for truncation (page 24, Section 4.2, paragraph 2, lines 1-4).

8. With respect to claims 4 and 10, Kim et al. disclose a method, wherein said filtering step outputs an event if the parameters indicate that ownership or group ownership of a file has been changed (page 24, Section 4.2, paragraph 2, lines 1-4).

9. With respect to claims 5 and 11, Kim et al. disclose a method, comprising a create step which outputs an alert message if a file was renamed including a file that was renamed and a new name that the file was renamed to (Table 2; page 27, Section 5.3, paragraph 2, lines 3-5; page 25, column 1, paragraph 1, lines 1-5).

10. With respect to claims 6 and 12, Kim et al. disclose a method, comprising configuring templates based on a list of files and directories to be included or excluded based on whether the files and directories are considered unmodifiable (page 24, column 1, Configurability and Flexibility Section, paragraph 3, lines 1-4).

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Rowland (U.S. Patent 6,405,318) also discloses the limitations of the independent claims and several of the dependent claims of the application. Moran (U.S. Patent 6,647,400) also discloses some of the independent and dependent claims in the invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ramya Ananthanarayanan whose telephone number is (571) 272-5860. The examiner can normally be reached on Monday through Friday, 8:30 -5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Ra

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER